UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,498	06/29/2001	James S. Magdych	NAI1P012/01.132.01	8154

28875 7590 10/25/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/895,498	**Applicant(s)** MAGDYCH ET AL.
	Examiner Eleni A. Shiferaw	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/9/2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-20 and 22-39* is/are pending in the application.

4a) Of the above claim(s) *3 and 21* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2,4-20 and 22-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Detailed Action

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 9, 2005 has been entered.

2. Claims 1-2, and 4-20, and 22-39 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5, 8-14, 18-23, 26-32, 36, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al. (Fox, Patent No.: US 6,883,101 B1) in view of Converse et al. (Converse, Pub. No.: US 2002/0143963 A1).

As per claims 1, 18, and 36, Fox teaches a method/program/system for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

(a) initiating a risk assessment scan on a target from a remote source utilizing a network (col. 3 lines 19-col. 4 lines 4, fig. 8B, and col. 6 lines 1-40; *network risk/vulnerability analyzer programs assessing risk on network nodes remotely*);

(b) determining whether the risk assessment scan on the target involves an intermediate device coupled between the target and the remote source (col. 4 lines 18-20; *different multiple programs of the analyzer analyzing if risky or vulnerable node connected to the network between the analyzer and authorized network node*);

(c) receiving results of the risk assessment scan from the target utilizing the network (col. 2 lines 56-63; *risk analysis result/survey filled out and transmitted to the risk analyzer by target/authorized network node)*; and

wherein additional operations are carried out to improve a risk assessment on the target in view of the presence of the intermediate device coupled between the target and the remote source (col. 11 and col. 12; *treats and improvements...*);

wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device (col. 6 lines 1-39 and col. 7 lines 42-46; *Fox discloses a method of multiple different risk analyzer tools, that have plurality of procedures, to be run against the same system remotely to analyze risk to network nodes and assesses if vulnerable node is connected to the network between the analyzer and authorized network node, and produce a more robust and accurate picture of a system's security posture. ANSSR, RAM, and ISS with plurality of procedures*).

Fox fails to explicitly teach notifying an administrator;

However **Converse** discloses (d) notifying an administrator if it is determined that the risk assessment scan on the target involves the intermediate device (par. [0025-0026]; *Converse discloses another procedure of assessing risk/unauthorized node/intermediate* *device connected on the network by comparing attack signature file/predetermined list with IP address of requestors and if IP address is not found on the list/positive it notifies the web server/administrator to take action*);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Converse within the system of Fox because they are analogous in network security assessment and identifying an authorized access or node (par. 0018). One would have been motivated to incorporate the teachings of Converse because it is well known to notify an administrator when unauthorized node is detected on the network (par. [025-0026]). Notifying an administrator would allow to take an action on the identified node/deny access.

As per claims 2, 19, and 39 Fox and Converse disclose all the subject matter as disclosed above. In addition Fox teaches a method/program, wherein the intermediate device includes a router (col. 6 lines 31-39, and col. 5 lines 32-42).

As per claims 4, and 22, Fox and Converse disclose all the subject matter as disclosed above. In addition, Converse teaches a method/program, wherein at least one of the procedures includes determining a port list associated with the risk assessment scan (par. 0025-0026). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention to use a procedure of port list associated with a risk assessment scan because it is well known. One would have been motivated to incorporate port list risk assessment method because combining multiple procedures would provide a better security.

As per claims 5, and 23, Fox and Converse disclose all the subject matter as disclosed above. In addition, Converse teaches a method/program, wherein the at least one of the procedures further includes determining whether a value of a flag is different for communication attempts using at least two ports on the port list (par. 0025-0026; if the value of the flag is positive/IP address is not on the list/different ...). The rational for combining are the same as claim 4 above.

As per claims 8, and 26, Fox and Converse disclose all the subject matter as disclosed above. In addition, Fox teaches a method/program, wherein the communications include connection attempts between the remote source and the target utilizing the network (col. 5 lines 47-53).

As per claims 9, and 27, Fox and Converse disclose all the subject matter as disclosed above. In addition, Converse teaches a method/program, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the value of the flag is different for the communication attempts using the at least two ports on the port list (claim 1 and 2; *if communication request IP address is different to the predetermined list, identifying the communication request node as unauthorized node/intermediate node*).

As per claims 10, and 28, Fox and Converse disclose all the subject matter as disclosed above. In addition, both teach a method/program, wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network (Fox col. 2 lines 56-64, and Converse par. 0023).

As per claims 11, and 29, Fox and Converse disclose all the subject matter as disclosed above. In addition, both teach a method/program, wherein the cached content is requested from the target utilizing a via tag (Fox col. 2 lines 56-64, and Converse par. 0023).

As per claims 12, and 30, Fox and Converse disclose all the subject matter as disclosed above. In addition, Fox teaches a method/program, wherein the at least one of the procedures further includes analyzing responses to the first and second requests (col. 2 lines 56-63).

As per claims 13, and 31, Fox and Converse disclose all the subject matter as disclosed above. In addition, Fox teaches a method/program, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis (col. 4 lines 18-20; *different multiple programs of the analyzer analyzing... risky or vulnerable node connected to the network between the analyzer and authorized network node*).

As per claims 14, and 32, Fox and Converse disclose all the subject matter as disclosed above. In addition, Fox teaches a method/program, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different (col. 4 lines 18-20; *different multiple programs of the analyzer analyzes... if risky or vulnerable node connected to the network between the analyzer and authorized network node in using user's survey*).

5. Claims 6-7, and 24-25 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al. (Fox, Patent No.: US 6;883,101 B1) in view of Converse et al. (Converse, Pub. No.: US 2002/0143963 A1), and Applicant Admitted Prior Art (AAPA).

As per claims 37 and 38, Fox teaches a computer program product/method for detecting modifications to risk assessment scanning caused by a proxy server, comprising:

(a) computer code for initiating a risk assessment scan on a target from a remote source utilizing a network (col. 4 lines 18-20; *different multiple programs of the analyzer analyzing if risky or vulnerable node connected to the network between the analyzer and authorized network node*);

(b) computer code for executing a plurality of procedures to determine whether the risk assessment scan on the target involves a proxy server coupled between the target and the remote source (col. 6 lines 1-39 and col. 7 lines 42-46; *Fox discloses a method of multiple different risk analyzer tools, that have plurality of procedures, to be run against the same system remotely to analyze risk to network nodes and assesses if vulnerable node is connected to the network between the analyzer and authorized network node, and* *produce a more robust and accurate picture of a system's security posture. ANSSR, RAM, and ISS with plurality of procedures*);

(e) computer code for flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source (col. 14 lines 60-col. 15 lines 2);

(d) computer code for receiving results of the risk assessment scan from the target utilizing the network (col. 2 lines 56-63; *risk analysis result/survey filled out and transmitted to the risk analyzer by target/authorized network node)*;

wherein additional operations are carried out to improve a risk assessment on the target in view of the presence of the proxy server coupled between the target and the remote source (col. 11 and col. 12; *treats and improvements*...).

Fox fails to explicitly teach notifying an administrator;

However **Converse** discloses (f) computer code for notifying an administrator if the results of the risk assessment scan on the target are flagged (par. [0025-0026]; *Converse discloses another procedure of assessing risk/unauthorized node/intermediate device connected on the network by comparing attack signature file/predetermined list with IP address of requestors and if IP address is not found on the list/flagged positive it notifies the web server/administrator to take action*);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Converse within the system of Fox because they are analogous in network security assessment and identifying an authorized access or node (par. 0018). One would have been motivated to incorporate the teachings of Converse because it is well known to notify an administrator when unauthorized node is detected on the network (par. [025-0026]). Notifying an administrator would allow to take an action on the identified node/deny access.

Fox and Converse do not explicitly teach (c) said procedures utilizing a plurality of parameters selected from the group consisting of an ip_ttl flag, a tcp-win flag, a via tag, and a host header value;

However AAPA discloses ip_ttl flag, and tcp_win flag as a well known (AAPA page 9 par. 4-page 10 par. 2).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of AAPA within the combination system of Fox and Converse because it would allow to determine unauthorized (intermediate) device by comparing the values of the flags. Data is sent to different nodes and tag values are compared. If the tag values are different identify the new node.

As per claims 6-7, and 24-25, Fox and Converse disclose all the subject matter as described above.

Fox and Converse do not explicitly teach wherein the flag includes ip_ttl flag, a tcp-win flag, a via tag, and a host header value;

However AAPA discloses ip_ttl flag, and tcp_win flag as a well known (AAPA page 9 par. 4-page 10 par. 2).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of AAPA within the combination system of Fox and Converse because it would allow to determine unauthorized (intermediate) device by comparing the values of the flags. Data is sent to different nodes and tag values are compared. If the tag values are different identify the new node.

6. Claims 15-17 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al. (Fox, Patent No.: US 6,883,101 B1) in view of Converse et al. (Converse, Pub. No.: US 2002/0143963 A1), and further in view of Miles et al. (Miles, Patent No.: US 6,886,044 B1).

As per claims 15, and 33, Fox and Converse disclose all the subject matter as described above. Fox and Converse do not disclose wherein a method/program, wherein at least one of the procedures includes transmitting a request without specifying a host header value. However Miles discloses displaying an error message when unidentified/unknown header value is received (col. 23 lines 66-col. 24 lines 17).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Miles within the system of Fox and Converse because it would identify the node that has unknown header value.

As per claims 16, and 34, Fox, Converse, and Miles teach all the subject matter as described above. In addition Miles teaches a method/program, wherein the at least one of the procedures further includes identifying an error message in response to the request (col. 23 lines 66-col. 24 lines 17).

As per claims 17, and 34, Fox, Converse, and Miles teach all the subject matter as described above. In addition Fox teaches a method/program, wherein the at least one of the procedures includes indicating that the risk assessment scan involves the intermediate device if the response includes the error message (col. 6 lines 1-39 and col. 7 lines 42-46).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

October 19, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100